

Rebecca Davis (SBN 271662)

rebecca@lozeaudrury.com

**LOZEAU DRURY LLP**

1939 Harrison, Suite 150

Oakland, CA 94612

Telephone: (510) 836-4200

Facsimile: (510) 836-4205

Patrick H. Peluso (admitted *pro hac vice*)

ppeluso@woodrowpeluso.com

Steven L. Woodrow (admitted *pro hac vice*)

swoodrow@woodrowpeluso.com

Taylor T. Smith

tsmith@woodrowpeluso.com (admitted *pro hac vice*)

**WOODROW & PELUSO, LLC**

3900 East Mexico Avenue, Suite 300

Denver, Colorado 80210

Telephone: (720) 213-0675

Facsimile: (303) 927-0809

*Attorneys for Plaintiff and the Class*

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

**Loretta Williams**, individually and on  
behalf of all others similarly situated,

Plaintiff,

v.

**DDR Media, LLC**, a Pennsylvania limited  
liability company, **d/b/a Royal Marketing  
Group**, and **Lead Intelligence, Inc.**, a  
Delaware corporation, **d/b/a Jornaya**

Defendants.

Case No. 3:22-cv-03789-SI

**PLAINTIFF'S COMBINED  
RESPONSE IN OPPOSITION TO  
DEFENDANTS' MOTIONS TO  
DISMISS**

Date: June 2, 2023

Time: 10:00 a.m.

Judge: Hon. Susan Illston

**TABLE OF CONTENTS**

**TABLE OF AUTHORITIES** ..... ii

**I. INTRODUCTION**.....1

**II. BACKGROUND** .....1

**III. ARGUMENT** .....2

**A. Plaintiff Has Adequately Stated Her Claims For Relief Against Defendants For Violation Of CIPA’s Wiretapping Prohibition** .....3

        1. Plaintiff’s communications were intercepted by Jornaya while in transmission to DDR.....4

        2. Plaintiff’s personal information was the intended message conveyed in the communication and, thus, the intercepted “contents” of her communication. ....6

        3. Jornaya’s involvement is akin to that of an eavesdropper, not merely a tape recorder. ....7

**B. Plaintiff Has Stated A Claim For Relief For Invasion Of Privacy Pursuant To The California Constitution.** .....13

**C. Plaintiff’s Allegation That Defendants Violated Her Privacy Rights Under CIPA Is Sufficient Harm To Support Standing** .....14

**IV. CONCLUSION** .....16

**TABLE OF AUTHORITIES**

<i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 544 (2007) .....	2
<i>Birdsong v. Apple, Inc.</i> , 590 F.3d 955 (9th Cir. 2009).....	2
<i>Conley v. Gibson</i> , 355 U.S. 41 (1957) .....	3
<i>Graham v. Noom, Inc.</i> , 533 F. Supp. 3d 823 (N.D. Cal. 2021) .....	8–9, 12
<i>Great Minds v. Off. Depot, Inc.</i> , 945 F.3d 1106 (9th Cir. 2019) .....	3
<i>Hart v. TWC Prod. &amp; Tech. LLC</i> , 526 F. Supp. 3d 592 (N.D. Cal. 2021) .....	13, 14
<i>In re Facebook, Inc. Internet Tracking Litigation</i> , 956 F.3d 539 (9th Cir. 2020) .....	3, 12, 13, 14
<i>In re Vizio, Inc., Consumer Priv. Litig.</i> , 238 F. Supp. 3d 1204 (C.D. Cal. 2017) .....	5
<i>In re Zynga Priv. Litig.</i> , 750 F.3d 1098 (9th Cir. 2014) .....	6
<i>Javier v. Assurance IQ, LLC</i> , No. 20-CV-02860-CRB, 2023 WL 114225 (N.D. Cal. Jan. 5, 2023) .....	9–11, 12
<i>Johnson v. Blue Nile, Inc.</i> , 2021 WL 1312771 (N.D. Cal. Apr. 8, 2021) .....	9
<i>Licea v. Cinmar, LLC</i> , No. CV 22-6454-MWF (JEM), 2023 WL 2415592 (C.D. Cal. Mar. 7, 2023) .....	5, 15
<i>Matera v. Google Inc.</i> , No. 15-CV-04062-LHK, 2016 WL 8200619 (N.D. Cal. Aug. 12, 2016) .....	3, 15
<i>Navarro v. Block</i> , 250 F.3d 729 (9th Cir. 2001) .....	2–3
<i>Osgood v. Main Streat Mktg., LLC</i> , Case. No. 16-cv-2415-GPC (BGS), 2017 WL 131829 (S.D. Cal. Jan. 13, 2017) .....	15
<i>Raffin v. Medicredit, Inc.</i> , No. 15-cv-4912-GHK-PJW, 2016 WL 7743504 (C D. Cal. Dec. 19, 2016) .....	15
<i>Revitch v. New Moosejaw, LLC</i> , No. 18-CV-06827-VC, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) .....	10, 14
<i>Ribas v. Clark</i> , 38 Cal. 3d 355, 696 P.2d 637 (1985) .....	10, 12
<i>Saleh v. Nike, Inc.</i> , 562 F. Supp. 3d 503 (C.D. Cal. 2021) .....	10

1	<i>Sanders v. Am. Broad. Cos.</i> , 20 Cal. 4th 907, 85 Cal.Rptr.2d 909, 978 P.2d 67 (1999) .....	13
2	<i>Smith v. LoanMe, Inc.</i> , 11 Cal. 5th 183 (2021) .....	12
3	<i>Tavernetti v. Superior Ct.</i> , 22 Cal. 3d 187, 583 P.2d 737 (1978) .....	9
4	<i>Underhill v. Kornblum</i> , No. 16-CV-1598-AJB-WVG,	
5	2017 WL 2869734 (S.D. Cal. Mar. 16, 2017) .....	5
6	<i>United States v. Reed</i> , 575 F.3d 900 (9th Cir. 2009) .....	6
7	<i>Williams v. What If</i> , 747 F.3d 733 (9th Cir. 2014) .....	3
8	<i>Yale v. Clicktale, Inc.</i> , 2021 WL 1428400 (N.D. Cal. Apr. 15, 2021) .....	9
9	<i>Yoon v. Lululemon USA, Inc.</i> , 549 F. Supp. 3d 1073 (C.D. Cal. 2021) .....	12
10	<b>STATUTES, RULES, SECONDARY SOURCES</b>	
11	Cal. Penal Code § 631, <i>et seq.</i> .....	<i>passim</i>

## I. INTRODUCTION

This case challenges Defendants DDR Media, LLC d/b/a Royal Marketing Group’s (“DDR”) and Lead Intelligence, Inc. d/b/a Jornaya’s (“Jornaya”) (collectively “Defendants”) violations of the California Invasion of Privacy Act, Cal. Penal Code 631 (“CIPA”). Specifically, Plaintiff alleges that Defendants have conspired and engaged in serial wiretapping of the electronic communications of visitors to DDR’s websites, violating CIPA and the California Constitution. In response to Plaintiff’s complaint, Defendants have each filed a motion to dismiss Plaintiff’s complaint for failure to state a claim. (Dkt. 47, 48.) However, none of the arguments presented in the motions wins the day—Plaintiff adequately states claims for relief against Defendants for violating CIPA by wiretapping communications. She alleges that Jornaya—a self-described “neutral, 3rd party witness”—intercepted her communications while they were being transmitted to DDR. Jornaya did so at DDR’s request, and its involvement is akin to a third-party eavesdropper who surreptitiously recorded the conversation between Plaintiff and DDR. As such, and as explained further below, the Court should deny the motions to dismiss filed by DDR and Jornaya in their entirety.

## II. BACKGROUND

On June 27, 2022, Williams filed her Complaint, alleging that DDR and Jornaya violated the CIPA by wiretapping Plaintiff’s communications on the DDR website and alleging that they thereby also violated California’s constitutional right to privacy and unfair competition law. (*See* Dkt. 1 at ¶¶ 1–3, 12–13.) As will be proven at the appropriate time following necessary discovery, Plaintiff seeks to certify a class action on behalf of all consumers who, like Plaintiff, made communications to DDR through its websites that were unlawfully intercepted or recorded without consent. (*Id.* ¶¶ 26–28.) To redress Defendants’ unlawful conduct, Plaintiff seeks statutory damages for herself and the class, as well as injunctive relief requiring Defendants to cease their practice of wiretapping electronic communications without consent. (*Id.* ¶ 27.)

On December 15, 2022, Defendants filed a joint motion to compel arbitration, which was

ultimately denied by the Court on February 28, 2023. (Dkt. 29, 36.) Several months later, and as noted in the Parties' Joint Case Management Statement, Plaintiff agreed to amend her complaint to clarify DDR's "d/b/a" name Royal Marketing Group. (Dkt. 39, 43.) On April 12, 2023, DDR filed its motion to dismiss for failure to state a claim and for lack of jurisdiction based on its contention that Plaintiff lacks standing (dkt. 47), and Jornaya filed its own motion to dismiss on April 13, 2023, largely mirroring DDR's arguments for failure to state a claim. (Dkt. 48.) Because Defendant's arguments overlap considerably, Plaintiff hereby files this joint response in opposition to both DDR and Jornaya's motions to dismiss.

### III. ARGUMENT

In their motions, Defendants ask the Court to dismiss each of Plaintiff's various claims. Both defendants contend that Plaintiff has failed to state a claim relief for any of the three claims in the complaint, and DDR further contends that Plaintiff has not suffered a "harm" to support standing for any claim. (Dkt. 47 at 3–12; Dkt. 48 at 3-10.) As explained below, Defendant's arguments for dismissal fail—Plaintiff has adequately stated claims for relief under California law<sup>1</sup>, and, in the event the Court finds that Plaintiff lacks allegations as to any particular claim for relief, Plaintiff should be granted leave to amend her complaint as necessary. Put simply, Defendants' motions to dismiss should be denied.

To survive a motion to dismiss, a complaint must contain sufficient factual allegations to state a claim for relief that is plausible on its face. *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "Factual allegations must be enough to raise a right to relief above the speculative level[.]" *Id.* at 555. In ruling on a motion to dismiss, the court's task is to test the legal sufficiency of claims: "a claim may be dismissed only if 'it appears beyond doubt that the plaintiff can prove no set of facts in support of his claim which would entitle him to relief.'" *Navarro v. Block*, 250

---

<sup>1</sup> With respect to Plaintiff's second cause of action, brought under California's Unfair Competition Law, CAL. BUS. PROF. CODE § 17200, et seq., Plaintiff concedes that she did not experience a loss of money or property to support standing for said claim. *See Birdsong v. Apple, Inc.*, 590 F.3d 955, 959 (9th Cir. 2009).

1 F.3d 729, 732 (9th Cir. 2001) (quoting *Conley v. Gibson*, 355 U.S. 41, 45–46 (1957)). In making  
 2 the determination, the court must accept all factual allegations and draw every reasonable  
 3 inference from those facts in favor of the non-moving party. *Id.*; *Great Minds v. Off. Depot, Inc.*,  
 4 945 F.3d 1106, 1109 (9th Cir. 2019).

5 **A. Plaintiff Has Adequately Stated Her Claims For Relief Against Defendants**  
 6 **For Violation Of CIPA’s Wiretapping Prohibition.**

7 The primary focus of Defendants’ motions is Plaintiff’s first cause of action: violation of  
 8 CIPA and the prohibition on wiretapping. Section 631(a) of CIPA prohibits a number of actions  
 9 relating to wiretapping. It contains four distinct clauses, each of which refers to a different  
 10 violation of the statute—defendants may not (1) “intentionally tap” or make an unauthorized  
 11 connection with a telegraph or telephone wire; (2) willfully and without consent “read or attempt  
 12 to read or learn” the contents of a message or communication while it is in transit; (3) “use or  
 13 attempt to use” any information so obtained; or (4) “aid, agree with, employ, or conspire” with  
 14 any person to do any of the actions above. CAL. PENAL CODE § 631(a). The “paramount objective  
 15 of the [Electronic Communications Privacy Act] is to protect effectively the privacy of  
 16 communications,” and CIPA’s language was drafted broadly to apply to wiretapping performed  
 17 with “any machine, instrument, or contrivance, or in any other manner,” and to communications  
 18 transmitted “over any wire, line, or cable.” *In re Facebook, Inc. Internet Tracking Litigation*, 956  
 19 F.3d 539, 608 (9th Cir. 2020).

20 Though the first clause expressly applies to the tapping of telegraph or telephone wires,  
 21 the remainder of Section 631(a) is not limited to phone lines. *See, e.g., Matera v. Google Inc.*, No.  
 22 15-CV-04062-LHK, 2016 WL 8200619, at \*21 (N.D. Cal. Aug. 12, 2016). Thus, Plaintiff alleges  
 23 that Jornaya violated the second prong of Section 631(a) by intercepting and learning the contents  
 24 of her communication with DDR, as well as allegations that DDR violated the fourth prong by  
 25 “partner[ing] with (and conspir[ing] with) Jornaya” to do so. (Dkt. 43 at ¶¶ 39–44.) Defendants  
 26 contend for various reasons that Williams’ CIPA claim cannot proceed, broadly seeking to  
 27

discredit the claim in three ways: (1) Jornaya argues that the real-time recording of Plaintiff's activity and submission on DDR's website did not qualify as "interception" of a communication "in transit" subject to CIPA; (2) Defendants claim that Jornaya's recording does not involve "contents" of communications made by Plaintiff; and (3) Defendants suggest that Jornaya's involvement should be considered akin to a tool or "tape recorder" used by DDR, rather than a third party eavesdropping on the conversation. As explained below, each of these arguments lacks weight, and Plaintiff has adequately stated a claim for relief under CIPA on which she should be permitted to proceed.

**1. Plaintiff's communications were intercepted by Jornaya while in transmission to DDR.**

The first basis by which Defendants seek dismissal of Plaintiff's CIPA claim is that there was supposedly no "interception" of a communication in transit passing through a wire or cable. Jornaya contends that the communications were not intercepted during transmission—according to Jornaya, it accessed Plaintiff's information "only *after* the information arrived at its intended destination (DDR Media's website)." (Dkt. 48 at 6–7) (emphasis in original). In light of Plaintiff's allegations, this argument falls apart.

Jornaya's assertion that there was no "interception" of communication while being sent is flawed. CIPA's second clause prohibits attempts to read or learn the contents of a communication "while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within [California]." CAL. PENAL CODE § 631(a). Here, Plaintiff has plainly alleged that, while she was transmitting her personal information to DDR, her keystrokes and clicks were being recorded by Jornaya, a third party to whom she was not transmitting her information. (*See* Dkt. 1 at ¶¶ 20–26.) Williams alleges that the recording and interception "began the moment [she] and other members of the alleged Class visited the webpage," and continued until at least the moment when she submitted the information that she had typed. (*Id.* ¶¶ 23, 24.) During the recording, Plaintiff was typing and attempting to communicate her information to



1 DDR, and her actions and the content of her communication were simultaneously being recorded  
 2 by Jornaya without her knowledge. Jornaya would have the Court believe that it did not access  
 3 her information until “*after* it had reached its destination,” but this assertion is plainly  
 4 contradicted by the recording of Plaintiff’s visit. (*See* Dkt. 48 at 6.) In the video provided, Jornaya  
 5 recorded several screens of Plaintiff typing information into the website, prior to the point at  
 6 which she would have clicked “CHECK LISTINGS” to submit the information to DDR. (Dkt. 43-  
 7 1 at 5.)<sup>2</sup> Put another way, Jornaya was eavesdropping and recording Plaintiff’s actions *while* she  
 8 was communicating her information to DDR, and *before* the information reached its destination  
 9 and intended recipient (which would have occurred after she clicked a button to submit).

10 Further, her allegations are factually distinguishable from the cases cited by Jornaya in  
 11 which real-time interception was not sufficiently alleged. For instance, in *In re Vizio*, the Court  
 12 found that, while plaintiffs “need not prove their theory of interception on a motion to dismiss,”  
 13 reliance on an “inscrutable graphic with no textual explanation” was insufficient to clear the  
 14 hurdle. *In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1228 (C.D. Cal. 2017).  
 15 Likewise, “using the word ‘intercept’ repeatedly . . . without the addition of specific facts” was  
 16 insufficient in *Licea*, and the plaintiff in *Underhill* failed to suggest contemporaneous acquisition  
 17 of emails while they were being sent, rather than “after they were stored” on an email server.  
 18 *Licea v. Cinmar, LLC*, No. CV 22-6454-MWF (JEM), 2023 WL 2415592, at \*10 (C.D. Cal. Mar.  
 19 7, 2023); *Underhill v. Kornblum*, No. 16-CV-1598-AJB-WVG, 2017 WL 2869734, at \*4 (S.D.  
 20 Cal. Mar. 16, 2017). Plaintiff’s allegations are decidedly more than what was present in each of  
 21 these cases: she plainly alleges that her visit was recorded from the moment she visited the  
 22 website, well before any information reached DDR or would have been stored on any server.  
 23 (Dkt. 43 at ¶¶ 20–26.) Williams’ contention that Jornaya’s recorded her visit “in real time” is not  
 24 conclusory—it is supported by her factual allegations and confirmed by the video itself.

---

25  
 26  
 27 <sup>2</sup> Recording available at <https://vp.leadid.com/playback/362C814B-AC01-2951-0637-0F1FF4511319?key=1639146863454> (last viewed Apr. 25, 2023).

1 Plaintiff claims that Defendants worked together to intercept her communications as she  
 2 made them to DDR, or “in real time.” She alleges that Jornaya intercepted the communications  
 3 while they were in the process of being sent to DDR, and she supports her claim by describing the  
 4 extent of the recording, which occurred from the moment she arrived on the site and while she  
 5 was communicating information to DDR, as well as providing a link to the recording hosted by  
 6 Jornaya. Her allegations are not conclusory—they are adequate to state a claim for relief, and  
 7 Jornaya’s motion to dismiss on this basis should be denied.

8 **2. Plaintiff’s personal information was the intended message conveyed in**  
 9 **the communication and, thus, the intercepted “contents” of her**  
 10 **communication.**

11 Defendants also argue that Plaintiff’s CIPA claim fails because they contend that the  
 12 information intercepted amounts only to record information, rather than the contents of Plaintiff’s  
 13 communication. Record information, as opposed to the contents of a message, is “data that is  
 14 incidental to the use of a communication device and contains no ‘content’ or information that the  
 15 parties intended to communicate.” *United States v. Reed*, 575 F.3d 900, 916 (9th Cir. 2009); *see*  
 16 *also In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014) (describing record information  
 17 as “information regarding the characteristics of the message that is generated in the course of the  
 18 communication”). Thus, whether a piece of data is record information is determined in relation to  
 19 the medium of communication, and it is distinct from the intended message. *Id.*

20 Defendants cite to several cases in which, for example, name, email address, and phone  
 21 number data were found to be record information. (Dkt. 47 at 7–8; Dkt. 48 at 8.) Such data can be  
 22 record information, particularly in cases regarding communications transmitted via phone or  
 23 email, but that is not the case here. As Plaintiff alleges, her communication with DDR consisted  
 24 of the submission and confirmation of Williams’ personal information in order to receive some  
 25 offering or “view listings.” (Dkt. 43 at ¶¶ 20–24; Dkt. 43-1 at 5.) Plaintiff’s personal information  
 26  
 27

1 and details included in the Jornaya’s video recording<sup>3</sup> were not “incidental” to her use of the  
 2 website—they were, in fact, the contents of her communication with DDR. The “record  
 3 information” incidental to her visit to the website, as noted in the complaint, include “the date and  
 4 time of the visit, her IP address, and her geographic location.” (Dkt. 43 at ¶ 21.) Plaintiff did not  
 5 intend to communicate that information to DDR; rather, it was generated as a result of the  
 6 medium of communication and merely detailed characteristics of her communication. Her  
 7 personal information—name, address, and phone number—was the content of her communication  
 8 with DDR and the message she intended to communicate. The mere fact that such types of data  
 9 may be record information in other cases does not necessarily make them so here. By Defendants’  
 10 logic, divulging personal information such as name or address could never be protected, even if it  
 11 were the sole content and purpose of a communication.

12 Defendants’ position is untenable. Phone numbers and email addresses may be record  
 13 information when related to phone calls and email exchanges, but they are not categorically  
 14 excluded from being “contents” of a communication. Plaintiff communicated with DDR, and the  
 15 content of her message included her name, zip code, email address, and phone number. The  
 16 record information in this instance was the date and time of her visit, IP address, and geographic  
 17 location—not the very information that she intended to convey to DDR. Accordingly,  
 18 Defendants’ arguments that only record information was recorded or intercepted is without merit.

19 **3. Jornaya’s involvement is akin to that of an eavesdropper, not merely a**  
 20 **tape recorder.**

21 Defendants further move for dismissal based on the argument that Jornaya supposedly  
 22 does not qualify as a third party that intercepted or tapped the communications between Plaintiff  
 23 and DDR—according to Defendants, Jornaya’s “TCPA Guardian” software should be treated akin  
 24 \_\_\_\_\_

25 <sup>3</sup> While Jornaya’s video recording censors the personal information that Plaintiff entered into the  
 26 form, its replay webpage enables a viewer to input personal information to verify a match,  
 27 confirming that such information was, in fact, read and collected during the interception. (*See*  
 Dkt. 43-1 at 5); <https://vp.leadid.com/playback/362C814B-AC01-2951-0637-0F1FF4511319?key=1639146863454> (last viewed Apr. 25, 2023).

1 to a party to the communications using a tape recorder, rather than a third-party eavesdropper.  
 2 (Dkt. 47 at 4–7, Dkt. 48 at 4–5.) Defendants’ argument is premised on logic that would nullify  
 3 both the third and fourth clauses of CIPA’s Section 631(a), and otherwise the issue of whether  
 4 Jornaya may be treated as a tape recorder or an eavesdropper is a factual question best answered  
 5 after discovery.

6 The fourth prong of Section 631(a) imposes liability on anyone who “aids, agrees with,  
 7 employs, or conspires with any person” to engage in “any of the acts or things” prohibited by the  
 8 other three prongs of the section. CAL. PENAL CODE § 631(a). Thus, if Jornaya may be held liable  
 9 for intercepting and willfully learning the contents of Plaintiff’s communication with DDR, then  
 10 DDR may be held liable for employing or conspiring with Jornaya to do so—this is the very  
 11 nature of Plaintiff’s CIPA claim. (Dkt. 1 at ¶¶ 41–43) (“[DDR] partnered with (and conspired  
 12 with) Jornaya to achieve the unlawful conduct described herein.”). Though Jornaya’s product  
 13 code was implemented on DDR’s website, Plaintiff has alleged sufficient details to demonstrate  
 14 that Jornaya is an independent third party that collects, stores, and processes the recordings at  
 15 issue. (*See id.* ¶¶ 5–12, 25) (“All TCPA Guardian videos are hosted on Jornaya’s servers, and to  
 16 access the videos one must follow a hyperlink provided by Jornaya. Moreover, Jornaya  
 17 independently collects and stores information provided by web users on the websites of its  
 18 clients.”) Further still, Jornaya’s own promotional materials describe the TCPA Guardian  
 19 platform as “a neutral, 3rd party witness to the events that take place on the website.” (Dkt. 43-1  
 20 at 3.) Taken as true, these factual allegations are sufficient to state a claim that Jornaya is liable as  
 21 an independent third party that intercepted Plaintiff’s communications (in violation of § 631(a)’s  
 22 second clause) and DDR is liable for agreeing or conspiring with Jornaya to do so (in violation of  
 23 § 631(a)’s fourth clause).

24 Defendants compare the facts of this case to a number of cases, like *Graham*, in support of  
 25 their contention that Jornaya is not a third party wiretapper but “merely a vendor” of software that  
 26 served only as an “extension of the website,” or “a tool used by a party, like a tape recorder.”  
 27

(Dkt. 47 at 4–5) (citing *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823 (N.D. Cal. 2021); *Johnson v. Blue Nile, Inc.*, 2021 WL 1312771 (N.D. Cal. Apr. 8, 2021); *Yale v. Clicktale, Inc.*, 2021 WL 1428400, at \*3 (N.D. Cal. Apr. 15, 2021); *Williams v. What If Holdings, LLC*, No. C 22-03780 WHA, 2022 WL 17869275 (N.D. Cal. Dec. 22, 2022). DDR goes further to describe Jornaya’s involvement to “the functional equivalent of video surveillance by a business owner” monitoring a physical store. (Dkt. 47 at 4.) These comparisons are flawed in several ways.

First, cases like *Graham* and *Williams* considered whether the plaintiff alleged that the third party “intercepted and used the data itself.” *Graham*, 533 F. Supp. at 823; *Williams*, 2022 WL 17869275, at \*3. But Section 631(a) imposes liability “for three distinct and mutually independent patterns of conduct: [1] intentional wiretapping, [2] willfully attempting to learn the contents or meaning of a communication in transit over a wire, and [3] attempting to use or communicate information obtained as a result of engaging in either of the previous two activities,” with a fourth basis of liability for agreeing or conspiring with another to do any of the above. *See Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192, 583 P.2d 737 (1978). In other words, a plaintiff need not plead usage of the information to state a claim under the second or fourth clauses of Section 631(a). In *Javier*, the Court recently decline to read an additional “use” requirement into the statute:

There are two problems with this reading of Section 631. The first is that it interprets the second prong of the statute—“willfully and without consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit”—based on the intentions and usage of the prospective third party. But the third prong of the statute already penalizes “use”—“us[ing], or attempt[ing] to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained.” Thus, **reading a use requirement into the second prong would add requirements that are not present (and swallow the**

1 **third prong in the process**). The second problem with this view is that it was not  
 2 the California Supreme Court’s stated rationale in *Ribas*: The *Ribas* Court did not  
 3 consider the wife’s friend’s intentions or the use to which they put the information  
 4 they obtained. Instead, it emphasized the privacy concerns at issue with having an  
 5 “unannounced second auditor” listening in on the call, when Section 631 concerns  
 6 “the right to control the nature and extent of the firsthand dissemination of [their]  
 7 statements.”

8 *Javier v. Assurance IQ, LLC*, No. 20-CV-02860-CRB, 2023 WL 114225, at \*6 (N.D. Cal. Jan. 5,  
 9 2023) (emphasis added) (internal citations omitted). An eavesdropper who is employed or  
 10 authorized by one party to intercept or record a communication is subject to liability, regardless of  
 11 any further use of the information. *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021)  
 12 (rejecting defendants’ argument “that any third party who surreptitiously recorded a conversation  
 13 between two parties would not violate § 631(a) so long as it was recording the conversation at the  
 14 direction and for the benefit of a party”) (citing *Revitch v. New Moosejaw, LLC*, No. 18-CV-  
 15 06827-VC, 2019 WL 5485330, at \*2 (N.D. Cal. Oct. 23, 2019) (“Although Moosejaw cannot be  
 16 liable for eavesdropping on its own communications with Revitch, the complaint adequately  
 17 alleges that Moosejaw violated section 631 by enabling [a third party’s] wrongdoing.”). Likewise,  
 18 the Court here should not consider further “use” of intercepted communications as a requirement  
 19 for determining that Jornaya was an unauthorized third-party eavesdropper rather than a tape  
 20 recorder.

21 DDR’s video surveillance analogy is similarly unavailing. Notwithstanding the obvious  
 22 factual disparities—including that website users often browse from the privacy of their home  
 23 rather than in public, and that video surveillance observes visible behavior as opposed to listening  
 24 in to the contents of a private conversation (and thus would not be actionable under CIPA)—a  
 25 video surveillance camera, like a tape recorder, is a physical tool, and it is incapable of exercising  
 26 control over or making any decisions as to the footage it captures. As outlined in *Javier*, this is a  
 27

1 useful distinction that critically does not read an additional “use” requirement into the second  
2 prong of Section 631(a):

3       There are only two other grounds upon which to conclude that ActiveProspect is  
4 not an “unannounced second auditor” of the interaction between Javier and  
5 Assurance: (1) If ActiveProspect does not have the **capability** to use its record of  
6 the interaction for any other purpose (just as a tape recorder has no independent  
7 capability to divulge the recording for any other purpose but that of its owner); or  
8 (2) the ubiquity of services like ActiveProspect on the internet effectively renders  
9 it party to the “firsthand dissemination” of Javier’s information to Assurance. As to  
10 the first, Javier pleads that ActiveProspect monitors, analyzes, and stores  
11 information about visits to Assurance’s websites, and that Active Prospect can use  
12 that information for other purposes, **even if Javier has not alleged that they have**  
13 **done so** in this case. . . . [T]his is “beyond the ordinary function of a tape recorder.”

14       As to the second, Javier pleads that he was “unaware at the time that his keystrokes,  
15 mouse clicks, and other electronic communications . . . would be disclosed to  
16 ActiveProspect,” and the Court treats this allegation as true on a motion to dismiss.

17 *Javier*, 2023 WL 114225, at \*6 (N.D. Cal. Jan. 5, 2023) (emphasis added) (internal citations  
18 omitted). The same analysis should apply here. Jornaya is capable of divulging its recordings  
19 independent of DDR’s purposes—as Plaintiff alleges, Jornaya hosts the recordings on its own  
20 servers, provides hyperlinks for third parties to access the recordings, and “independently collects  
21 and stores information provided by web users on the websites of its clients.” (*See* Dkt. 43 at ¶ 25.)  
22 Jornaya even states in its materials that it provides such recordings to “[c]ompanies that purchase  
23 3rd party data leads,” as opposed to the companies that obtain lead information directly from  
24 consumers, *i.e.*, the actual parties to the communication. (Dkt. 43-1 at 3.) Plaintiff also alleges  
25 that she did not know her communications were being recorded: the recording “was done without  
26 Plaintiff’s consent,” and Defendants “did not inform” Williams or other visitors of the recording,  
27



1 as it began the moment they arrived at the website. (*See* Dkt. 43 at ¶ 24.) Just as the Court deemed  
 2 these allegations sufficient in *Javier*, Plaintiff has alleged sufficient facts to suggest that Jornaya  
 3 was a third-party eavesdropper to her communication with DDR, not merely a tape recorder.

4 The California Supreme Court has often emphasized the “express objective” of CIPA—to  
 5 protect a person making communications from a situation where the person on the other end of  
 6 the line “permits an outsider to . . . listen in.” *Ribas v. Clark*, 38 Cal. 3d 355, 364, 696 P.2d 637  
 7 (1985); *see also Smith v. LoanMe, Inc.*, 11 Cal. 5th 183, 200 (2021) (noting distinction between  
 8 secondhand repetition of a conversation and “simultaneous dissemination to an unannounced  
 9 second auditor, whether that auditor be a person or mechanical device”). The Ninth Circuit has  
 10 similarly held that wiretapping statutes are designed “to prevent the acquisition of the contents of  
 11 a message by an unauthorized third-party or ‘an unseen auditor.’” *In re Facebook*, 956 F.3d 589,  
 12 608 (9th Cir. 2020). Plaintiff recognizes that, as pointed out by Defendants, several decisions in  
 13 this Court and others have rested upon whether the alleged third party “used” the data in some  
 14 way, even though this constitutes its own separate violation of CIPA. *Compare, e.g., Graham*,  
 15 533 F. Supp. at 823; *Williams*, 2022 WL 17869275, at \*3; *with Javier*, 2023 WL 114225, at \*6.  
 16 Under the *Javier* standard, Plaintiff has alleged sufficient facts to state claims for relief under two  
 17 clauses of Section 631(a), regardless of whether Jornaya “used” her information in some yet  
 18 unidentified way. Nevertheless, should the Court here elect to follow the opposing trend to  
 19 “swallow the third prong” by reading a use requirement into the second prong of CIPA, Plaintiff  
 20 requests an opportunity to amend her complaint accordingly.

21 Ultimately, the issue of whether Jornaya is more appropriately likened to a tape recorder  
 22 or an eavesdropper “is a question of fact for a jury, best answered after discovery into the storage  
 23 mechanics of” its system. *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1081 (C.D. Cal.  
 24 2021). At the pleadings stage, Plaintiff has met her burden to allege violations of CIPA above the  
 25 speculative level. Taken in a light most favorable to the Plaintiff, as must be done a motion to  
 26 dismiss, Plaintiff’s allegations adequately state claims for relief under CIPA, and Defendants’  
 27



1 motions to dismiss should be denied.

2 **B. Plaintiff Has Stated A Claim For Relief For Invasion Of Privacy Pursuant To**  
 3 **The California Constitution.**

4 In addition to arguing that Williams failed to state a claim for violations of CIPA,  
 5 Defendants contend that Plaintiff has not adequately stated a claim for invasion of privacy under  
 6 the Constitution of California. To plead a privacy violation under the California Constitution, a  
 7 plaintiff must allege (1) a legally protected privacy interest, (2) a reasonable expectation of  
 8 privacy, and (3) an intrusion constituting an egregious breach of social norms. *Hart v. TWC Prod.*  
 9 *& Tech. LLC*, 526 F. Supp. 3d 592, 600 (N.D. Cal. 2021) (quoting *In re Facebook*, 956 F.3d at  
 10 601 (9th Cir. 2020)). The analysis is often simplified to two elements: “(1) there exists a  
 11 reasonable expectation of privacy, and (2) the intrusion was highly offensive.” *Hart*, 526 F. Supp.  
 12 3d at 600. The existence of a reasonable expectation of privacy requires “examination of customs,  
 13 practices, and physical settings,” as well as “the opportunity to be notified in advance and consent  
 14 to the intrusion.” *Id.* Expectations of privacy are nuanced and not absolute—for instance, “[t]he  
 15 mere fact that a person can be seen by someone does not automatically mean that he or she can  
 16 legally be forced to be subject to being seen by everyone.” *Id.* (quoting *Sanders v. Am. Broad.*  
 17 *Cos.*, 20 Cal. 4th 907, 916, 85 Cal.Rptr.2d 909, 978 P.2d 67 (1999)). The question of degree of  
 18 intrusion is similarly nuanced, but, while the qualification of “highly offensive” or “egregious”  
 19 may be seen as a high bar, the ultimate question of whether a given action ‘could highly offend a  
 20 reasonable person is an issue that cannot be resolved at the pleading stage.’” *Hart*, 526 F. Supp.  
 21 3d at 602 (quoting *In re Facebook*, 956 F.3d at 606).

22 Here, Plaintiff has alleged a reasonable expectation of privacy surrounding her browsing  
 23 activities and dissemination of personal information, including the expectation that she may do so  
 24 “without observation or interference” and “without being subjected to secret wiretaps.” (Dkt. 43  
 25 at ¶ 55.) Williams’ decision to share her information with DDR to take advantage of an offering  
 26 does not amount to a decision to share her information with everybody, nor does it anticipate or  
 27

1 authorize the employment of a third-party eavesdropper to record her keystrokes, mouse  
 2 movements, and personal information. Further, DDR could have notified website visitors that  
 3 their visit would be recorded and properly obtained consent before Jornaya began recording, but  
 4 no such notice was provided—instead, the recording began “the moment” Plaintiff reached the  
 5 website, with no indication whatsoever. (*See id.* ¶ 24.) Plaintiff has also alleged that Defendants’  
 6 conduct, and the practice of engaging unknown auditors to secretly monitor user activity on a  
 7 website and record personal information, is “serious in nature” and should be seen as an egregious  
 8 breach of social norms. (*See id.* ¶ 57.) Defendants cite to several cases in which certain internet  
 9 privacy invasions did not amount to a violation of the California Constitution, but there are  
 10 likewise several cases in this District where allegations of surreptitious monitoring of various  
 11 internet browsing activity and history were sufficient to state a claim for invasion of privacy. *See,*  
 12 *e.g., Hart*, 526 F. Supp. 3d at 600–03 (monitoring of location data by weather app); *Revitch*, 2019  
 13 WL 5485330, at \*3 (monitoring of mouse clicks, keystrokes, identity and browsing data); *see also*  
 14 *In re Facebook*, 956 F.3d at 601–06 (compiling of personalized profiles from browsing histories  
 15 and habits).

16 Defendants disagree that the alleged real-time interception of Williams’  
 17 communications—including monitoring keystrokes and mouse movements and recording identity  
 18 information—constitutes an “egregious” breach of social norms, but the issue cannot and should  
 19 not be resolved at the pleadings stage. *In re Facebook*, 956 F.3d at 606. Plaintiff has met her  
 20 burden to plead her constitutional claim above the speculative level, and her factual allegations,  
 21 taken as true, support the reasonable inference that Defendants committed an invasion of privacy  
 22 that is actionable under the California Constitution. Accordingly, the Court should deny  
 23 Defendants’ motions to dismiss and permit Plaintiff to proceed on her claim.

24 **C. Plaintiff’s Allegation That Defendants Violated Her Privacy Rights Under**  
 25 **CIPA Is Sufficient Harm To Support Standing.**

26 As a final note, DDR briefly moves for dismissal based on lack of subject matter  
 27

jurisdiction, claiming that Plaintiff lacks Article III standing to bring her claims for violation of CIPA. (Dkt. 47 at 10–11.) DDR contends that Williams’ claim amounts to “merely an injury in law” as opposed to an injury in fact, and it further claims that any harm she suffered is “akin to the harm suffered by someone who is captured on video surveillance in a convenience store buying soda, none.” (*Id.*) This argument is also unavailing.

Leaving aside DDR’s flawed attempt to again liken the facts of this case to video surveillance in a store, CIPA creates tangible privacy rights for individuals, and an allegation that those rights have been violated amounts to an injury in fact sufficient to confer standing:

“[V]iolations of [p]laintiffs’ statutory rights under CIPA, [even] without more, constitute injury in fact because instead of a bare technical violation of a statute, . . . a CIPA violation involves . . . a violation of privacy rights.” *Osgood v. Main Street Mktg., LLC*, Case. No. 16-cv-2415-GPC (BGS), 2017 WL 131829, at \*7 (S.D. Cal. Jan. 13, 2017) (internal citation omitted); *see also Raffin v. Medicredit, Inc.*, No. 15-cv-4912-GHK-PJW, 2016 WL 7743504, at \*3 (C D. Cal. Dec. 19, 2016) (“Following *Spokeo*, district courts in the Ninth Circuit consistently have concluded that, to satisfy injury in fact, a plaintiff in a CIPA action need not allege actual harm beyond the invasion of the private right conferred by the statute.”); *Matera v. Google Inc.*, Case No. 15-cv-04062-LHK, 2016 WL 5339806, at \*11 (N.D. Cal. Sept. 23, 2016) (denying motion to dismiss holding that alleged violations of plaintiff’s statutory rights under CIPA constitute concrete injury in fact under *Spokeo*).

*Licea*, 2023 WL 2415592, at \*3. Thus, the Court in *Licea* found the claim that the defendant “did not inform Plaintiffs, or any of the Class Members, that Defendant was secretly recording their communications or aiding, abetting, and paying third parties to eavesdrop on them” was sufficient to allege a CIPA violation and, therefore, an injury in fact to support standing. The same is true here—Plaintiff has alleged that “Defendants did not inform website visitors that their strokes and

clicks would be recorded, much less secure prior express consent” before DDR “partnered with and conspired with Jornaya” to eavesdrop on the communications and violate Plaintiff’s and the Class Members’ privacy rights established by CIPA. (*See* Dkt. 43 at ¶¶ 24, 41–43.) The harm alleged by Plaintiff is not merely an “injury in law,” but an injury in fact sufficient to give her standing to bring her CIPA claim against Defendants. DDR’s motion to dismiss should be denied on this basis as well.

#### IV. CONCLUSION

Defendants’ motions to dismiss Plaintiff’s claims should be denied. Plaintiff has met her burden to plead her claims for relief under both Section 631(a) of CIPA and the California Constitution above the speculative level. Jornaya intercepted her communication while it was in transit to DDR, it read and learned the contents of said communication, and its role is more akin to that of a third-party eavesdropper than a tape recorder because it is capable of independently controlling the dissemination of its recordings. Plaintiff has likewise alleged a highly offensive invasion of her reasonable expectation of privacy, and she has standing to bring her claims. To the extent the Court intends to read a “use” requirement into the second prong of Section 631(a), Plaintiff requests that she be granted leave to amend accordingly. However, the Court should deny Defendants’ motions, permit the parties to proceed, and award any such relief as it deems necessary and just.

Respectfully submitted,

Dated: April 26, 2023

**LORETTA WILLIAMS**, individually and on behalf of all others similarly situated,

By: /s/ Patrick H. Peluso

Rebecca Davis (SBN 271662)  
rebecca@lozeaudrury.com  
**LOZEAU DRURY LLP**  
1939 Harrison, Suite 150  
Oakland, CA 94612  
Telephone: (510) 836-4200  
Facsimile: (510) 836-4205

Patrick H. Peluso\*  
ppeluso@woodrowpeluso.com  
Steven L. Woodrow\*  
swoodrow@woodrowpeluso.com  
**WOODROW & PELUSO, LLC**  
3900 East Mexico Avenue, Suite 300  
Denver, Colorado 80210  
Telephone: (720) 213-0676  
Facsimile: (303) 927-0809

*Attorneys for Plaintiff and the Class*

*\* Pro Hac Vice*

**CERTIFICATE OF SERVICE**

The undersigned hereby certifies that a true and accurate copy of the above titled document was served upon counsel of record by filing such papers via the Court's ECF system on April 26, 2023.

/s/ Patrick H. Peluso